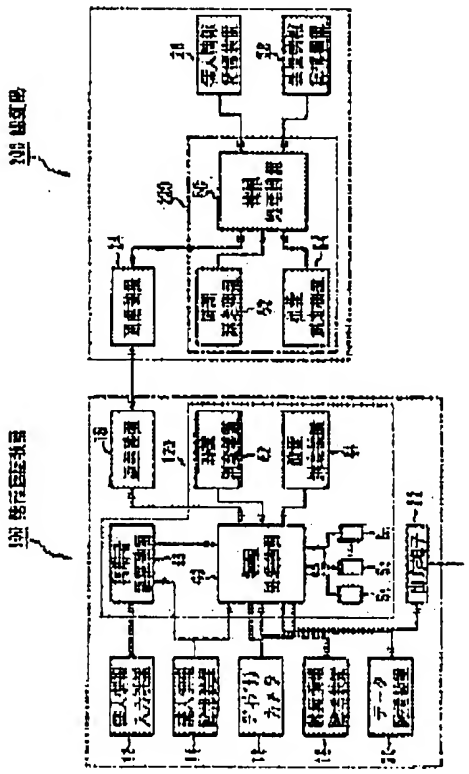
P12

(1)

INFORMATION AUTHENTICATION DEVICE AND AUTHENTICATION OFFICE

Patent number: JP2001100632 (A)
Publication date: 2001-04-13
Inventor(s): KOBAYASHI MICHIO
Applicant(s): SEIKO EPSON CORP
Classification:
- international: ***G09C1/00; G09C5/00; H04L9/32;*** **G09C1/00; G09C5/00; H04L9/32;** (IPC1-7): G09C1/00; H04L9/32
- european:
Application number: JP19990280825 19990930
Priority number(s): JP19990280825 19990930

Abstract of **JP 2001100632 (A)**
PROBLEM TO BE SOLVED: To provide an authentication device and an authentication office suitable for improving a verification ability as an evidence of data by ensuring objectivity of the data. SOLUTION: The information authentication device 100 is comprises of a digital camera 10, and an authentication information adding part 120 for adding authentication information to digital data. On the other hand, the authentication office 200 is provided with communication equipment 24 for receiving the digital data from the information authentication device 100 and a digital signature adding part 220, and when the digital signature adding part 220 authenticates that the digital data are inputted with the digital camera 10, based on the authentication information added to the digital data received by the communication equipment 24, it adds a digital signature to the digital data received with the communication device 24.



20/31

--- omission ---

[0086]

[Embodiments] An embodiment of the present invention is now explained with reference to the accompanying drawings. Fig. 1 to Fig. 5 show the configurations of an information authentication device and an authentication authority according to the present invention.

[0087] In this embodiment, as shown in Fig. 1, the information authentication device and the authentication authority of the present intention are applied to a case where digital data as a digital image taken by a digital camera 10 is authenticated.

[0088] First, a configuration of an information authentication system to which the information authentication device and the authentication authority of the present invention are applied is now explained with reference to Fig. 1. Fig. 1 is a block diagram illustrating a configuration of the information authentication system.

[0089] As shown in Fig. 1., this information authentication system is configured to include a digital authentication 200 for executing digital signature and an information authentication device 100 being connected via a network so that they can communicate with each other. The information authentication device 100 is not always connected to the authentication authority 200, for example, and connected to the authentication authority 200 only when digital data is to be authenticated. It is to be noted that the figure shows only one unit of the information authentication device 100 for convenience of interpretation of this invention, but in fact a plurality of different information authentication devices can be connected to the authentication authority 200.

[0090] The information authentication device 100 is composed of a digital camera 10 for taking digital data as a digital image, a personal information input device 12 for inputting personal information, a personal information memory unit 14 for storing personal information, a device information memory unit 16 for storing device information as information unique to the information authentication device 100, an authentication information adding section 120 for adding authentication information for authenticating that the digital data was taken by the digital camera 10, to the digital data taken by the digital camera 10, a communication device 18 for communicating with the authentication authority 200 via a network, a data memory unit 20 for storing the digital data with digital signature added by the authentication authority 200, and an output terminal 22 for outputting the digital data of the digital memory unit 20 outside.

[0091] The personal information inputting device 12 consists of an input device such as a keyboard. The personal information inputting device 12 is configured to input an ID allocated to each user of the information authentication device 100, and a password corresponding to the ID.

[0092] The personal information memory unit 14 stores encrypted personal information that is obtained by encrypting the ID allocated to each user of the information authentication devise 100 and the password corresponding to the ID. It is to be noted that the ID and the password are encrypted by using a personal ID encryption algorithm in the authentication authority 200.

[0093] The device information memory unit 16 stores encrypted device information that is obtained by encrypting device information as information unique to the information authentication device 100 (e.g., a number unique to a device). It is to be noted that the device information is information encrypted by using a device encryption algorithm.

[0094] The communication device 18 is configured to specify the nearest base station from

the present location by using a mobile phone, a PHS, or the like, link to a network via a general public line network by radio, and then transmit digital data via the network to the authentication authority 200.

[0095] A configuration of the authentication information adding section 120 is now explained more in detail.

[0096] The authentication information adding section 120 is composed of a time measuring device 42 for measuring a time, a location measuring device 44 for measuring a location, a plurality of sensor S_1 to S_n for measuring surrounding environmental conditions, a user authentication device 46 for conducting a user authentication by checking the personal information inputted through the personal information inputting device 12 against the personal information of the personal information memory unit 14, and an information processing device 40 for generating authentication information and adding this authentication information to the digital data taken by the digital camera 10.

[0097] The time measuring device 42 is configured to receive a time signal from an orbiting satellite transmitting a time signal indicating the present time, and measure the present time based on the received time signal.

[0098] The location measuring device 44 is configured to receive a time signal from an orbiting satellite transmitting the time signal indicating the present time, and measure the location of the present site based on a time lag indicated by those time signals and the orbit of each orbiting satellite, and with reference to the so called GPS for measuring a location.

[0099] The plurality of sensors S_1 to S_n is configured to measure surrounding environmental conditions, such as surrounding temperatures, humidity, atmospheric pressure, gas concentration, wind velocity, altitude, sound volume, and light volume, for example. A known measuring instrument can be used as the sensor for measuring those physical quantities.

[0100] The user authentication device 46 is configured to input an ID and a password by the personal information inputting device 12, upon receipt of a user's request for authentication from the information processing device 40, then at the same time, read out encrypted personal information from the personal information memory unit 14 to decrypt the encrypted personal information, and then determine whether or not the inputted ID and password matches the decrypted ID and password. As a determination result, if it is determined that these items of data match, then the user authentication device 46 outputs user authentication data indicating an authorized user to the information processing device 40. If it is determined that these items of data do not match, then the user authentication device 46 outputs user authentication data indicating an unauthorized user to the information processing device 40.

[0101] A configuration of the information processing device 40 is now explained with reference to Fig. 2. Fig. 2 shows a block diagram illustrating a configuration of the information processing device 40.

[0102] As shown in Fig. 2, the information processing device 40 is composed of a CPU 60 for operating and controlling the whole system based on a control program, a ROM 62 for storing in advance the CPU 60 control program and the like in a predetermined area, a RAM 64 for storing data read out from the ROM 62 and so forth and operation results required in the operation process of the CPU 60, and an I/F 68 for mediating the input/output of data for an external device. These devices are linked to one another via a bus 69 as a signal line for transferring data so that they can communicate data.

[0103] The I/F 68 is linked to such external devices as the digital camera 10, the personal

information memory unit 14, the device information memory unit 16, the communication device 18, the data memory unit 20, the output terminal 22, the time measuring device 42, the location measuring device 44, the sensors S_1 to S_n and the user authentication device 46.

[0104] The CPU 60 consists of micro processing unit MPU and so forth. The CPU 60 is configured to run a predetermined program stored in a predetermined area of the ROM 62 when the electric power is supplied, and execute an authentication information adding process illustrated in a flow chart shown in Fig. 3 according to the program. Fig. 3 is a flowchart illustrating the authentication information adding process.

[0105] In the authentication information adding process, the authentication information is generated by using an external device linked to the I/F 68, the generated authentication information is added to the digital data taken by the digital camera 10. When executed on the CPU 60, as shown in Fig. 3, the authentication information adding process starts from Step S100.

[0106] In Step S100, a user's request for authentication is outputted to the user authentication device 46, and the process proceeds to Step S102. In Step S102, the user authentication data is inputted from the user authentication device 46, and it is determined whether or not the inputted user authentication data indicates the authorized user. If it is determined that the inputted user authentication data indicates the authorized user (Yes), then the process proceeds to Step S104.

[0107] In Step S104, it is determined whether or not the digital data as a digital image is inputted from the digital camera 10. If it is determined that the digital data is inputted (Yes), then the process proceeds to Step S106. In Step S106, the present time is inputted from the time measuring device 42, time information to specify the point of time when the digital data was inputted by the digital camera 10 is generated based on the inputted time, and then the process proceeds to Step S108.

[0108] In Step S108, the location of the present spot is inputted from the location measuring device 44, generates the location information to specify the location of the spot where the digital data was inputted by the digital camera 10 is generated based on the inputted location, and then the process proceeds to Step S110. In Step S110, the surrounding environmental conditions are inputted through the sensors S_1 to S_n, then the environmental condition information to specify the environmental condition at the specific point of time when the digital data was inputted through the digital camera 10 is generated based on the inputted environmental condition, and then the process proceeds to Step S112.

[0109] In Step S112, the personal information is read out from the personal information memory unit 14, and then the process proceeds to Step S114. In Step S114, the device information is read out from the device information memory unit 16, and the process proceeds to Step S116. In Step S116, generated time information, generated location information, generated environmental condition information, readout personal information, and readout device information are added to the digital data inputted through the digital camera 10 as the authentication information, and the process proceeds to Step S108. More specifically, in Step S116, the authentication information is added to the digital data as electronic watermark or subliminal information, for example.

[0110] In Step S118, the digital data with the authentication information added is substituted into a predetermined hash function, thereby generating the test information to test whether or not the digital data includes an error, as a hash value determined by the hash function, and

then the process proceeds to Step S120. In Step S120, the digital data inputted by the digital camera 10 is further added with the generated test information as the authentication information, and then the process proceeds to Step S122. More specifically, in Step S122, the authentication information is added to the digital data as electronic watermark or subliminal information, for example.

[0111] In Step S122, the digital data with the authentication information added is encrypted with a secret key of the information authentication device 100 by the public key encryption system, and then the process proceeds to Step S124. In Step S124, the encrypted digital data is outputted to the communication device 18 to be transmitted to the authentication authority 200, and the process proceeds to Step S126.

[0112] In Step S126, it is determined whether or not the digital data with digital signature added by the authentication authority 200 is received and inputted through the communication device 18. If it is determined that the digital data with digital signature added is inputted (Yes), then the process proceeds to Step S128. In Step S128, the inputted digital data is stored in the data memory unit 20, and then the process proceeds to Step S130.

[0113] In Step S130, it is determined whether or not a request for outputting the digital data is issued from any user. If it is determined that a request for outputting the digital data is issued (Yes), then the process proceeds to Step S132. In Step S132, the digital data in the data memory unit 20 is outputted to the output terminal 22, and the process then proceeds to Step S104.

[0114] If it is determined in Step S130, on the other hand, that a request for outputting the digital data is not issued from any user (No), then the process proceeds to Step S104.

[0115] If it is determined in Step S126, on the other hand, that the digital data with digital signature added is not inputted through the communication device 18 (No), then the process remains in Step S126 until the digital data is inputted.

[0116] If it is determined in Step S104, on the other hand, that the digital data is not inputted through the digital camera 10 (No), then the process proceeds to Step S130.

[0117] If it is determined in Step S102, on the other hand, that the user authentication data indicates an unauthorized user (No), then the process proceeds to Step S134 where the electric power supply is forcibly shut off and thereby a series of operations is terminated.

[0118] A configuration of the authentication authority 200 is now explained with reference back to Fig. 1.

[0119] As shown in Fig. 1, the authentication authority 200 is composed of a communication device 24 for communicating with the information authentication device 100 via a network, a personal information memory unit 26 for storing the personal information, a device information memory unit 28 for storing the device information, and a digital signature adding section 220 for adding digital signature to the digital data received at the communication device 24.

[0120] The personal information memory unit 26 stores IDs and passwords identical to those stored in the personal information memory unit 14. More specifically, each of the identical IDs is allocated to a user using the information authentication device specified by the device information of the device information memory unit 28. The identical IDs correspond to the respective passwords. The personal information of the personal information memory unit 26 is correlated with the device information of the device information memory unit 28. More specifically, this correlation allows for the specification of the ID and password of a user of the information authentication device specified by the device information of the device

information memory unit 28. It is to be noted that this correlation process is implemented if a user who is to use the information authentication device 100 notifies the authentication authority 200 prior to the use of the information authentication device 100.

[0121] A configuration of the digital signature adding section 220 is now explained more in detail.

[0122] The digital signature adding section 220 is composed of a time measuring device 52 for measuring time, a location measuring device 54 for measuring the location of the information authentication device 100, and an information processing device 50 for adding digital signature to the digital data received through the communication device 24.

[0123] The time measuring device 52 is configured to have the same function as that of the time measuring device 42. The time measuring device 52 is configured to receive a time signal from an orbiting satellite transmitting a time signal indicating the present time, and measure the present time based on the received time signal.

[0124] The location measuring device 54 is configured to measure the location of the information authentication device 100 during a communication performed between the communication device 24 and the information authentication device 100, by specifying a base station which the information authentication device 100 is communicating with. It is to be noted that a conventional method is used to specify a base station.

[0125] A configuration of the information processing device 50 is now explained with reference to Fig. 4. Fig. 4 shows a block diagram illustrating a configuration of the information processing device 50.

[0126] As shown in Fig. 4, the information processing device 50 consists of a CPU 70 for operating and controlling the whole system based on a control program, a ROM 72 for storing the control program of the CPU 70 and so forth in advance in a predetermined area, a RAM 74 for storing data read out from the ROM 72 and so forth and operation results required in the operation process of the CPU 70, and an I/F 78 for mediating the input/output of data for an external device. These devices are linked to one another via a bus 79 as a signal line for transferring data so that they can communicate data.

[0127] The I/F 78 is linked to external devices such as the communication device 24, the personal information memory unit 26, the device information memory unit 28, the time measuring device 52, and the location measuring device 54.

[0128] The CPU 70 consists of micro processing unit MPU and so forth. The CPU 70 is configured to run a predetermined program stored in a predetermined area of the ROM 72, and execute a digital signature adding process illustrated in a flow chart shown in Fig. 5 according to the program on a steady basis. Fig. 5 is a flow chart illustrating the digital signature adding process.

[0129] In the digital signature adding process, digital signature is added to the digital data received through the communication device 24. As shown in Fig. 5, when executed on the CPU 70, the digital signature adding process starts from Step S200.

[0130] In Step S200, digital data is received from the information authentication device 100, and then it is determined whether or not the digital data is inputted through the communication device 24. If it is determined that the digital data is inputted (Yes), then the process proceeds to Step S202. In Step S202, the inputted digital data is decrypted with a public key of the information authentication device 100 as the transmitting source of the digital data, and the process then proceeds to Step S204.

[0131] In Step S204, the present time is inputted from the time measuring device 52, and then it is determined whether or not a time lag between the time specified by the time information added to the decrypted digital data as the authentication information and the time inputted from the time measuring device 52 is within a predetermined range (e.g., one minute). If it is determined that the time lag is within the predetermined range (Yes), then the process proceeds to Step S206.

[0132] In Step S206, the location of the information authentication device 100 as the transmitting source of the digital data is inputted from the location measuring device 54, and then it is determined whether or not the location specified by the location information added to the decrypted digital data as the authentication information is included in an area within a predetermined range (e.g., 300m in radius) with the location inputted from the location measuring device 54 as the center. If it is determined that it is included in the area within the predetermined range (Yes), then the process proceeds to Step S208.

[0133] In Step S208, the added device information as the authentication information of the decrypted digital data is decrypted, and the process proceeds to Step S210. In Step S210, the device information memory unit 28 is searched based on the decrypted device information, and the process then proceeds to Step S212. In Step S212, it is determined whether or not the device information corresponding to the decrypted device information is retrieved. If it is determined that the corresponding device information is retrieved (Yes), then the process proceeds to Step S214.

[0134] In Step S214, the personal information added as the authentication information of the decrypted digital data is decrypted, and then the process proceeds to Step S216. In Step S216, the personal information memory unit 26 is searched to retrieve corresponding personal information based on the retrieved device information in Step S212, and then the process proceeds to Step S218. In Step S218, it is determined whether or not the ID and password as the decrypted personal information matches the ID and password as the retrieved personal information. If it is determined that they match (Yes), then the process proceeds to Step S220.

[0135] In Step S220, most part of the decrypted digital data, except for the test information added as the authentication information, is substituted into the same hash function as that of Step S118, thereby generating the test information to test whether or not the digital data includes an error, as a hash value determined by the hash function, and the process then proceeds to Step S222. In Step S222, it is determined whether or not the generated test information matches the test information added as the authentication information of the decrypted digital data. If it is determined that they match (Yes), then the process proceeds to Step S224.

[0136] In Step S224, digital signature is added to the decrypted digital data, and the process then proceeds to Step S226, In Step S226, the digital data with the digital signature added is encrypted with a secret key of the authentication authority 200, and the process then proceeds to Step S228. In Step S228, the encrypted digital data is outputted to the communication device 24, then transmitted to the information authentication device 100 as the transmitting source, and the process then proceeds to Step S200.

[0137] If it is determined in Step S222, on the other hand, that the test information generated by the hash function and the test information added as the authentication information of the decrypted digital data do not match (No), then the digital data is regarded as unauthorized

data and therefore digital signature is not added thereto, and the process then proceeds to Step S200.

[0138] If it is determined in Step S218, on the other hand, that the ID and password as the decrypted personal information does not match the ID and password as the readout personal information (No), then the digital data is regarded as unauthorized data, and therefore digital signature is not added thereto, and the process then proceeds to Step S200.

[0139] If it is determined in Step S212, on the other hand, that the device information corresponding to the decrypted device information is not retrieved from the device information memory unit 28 (No), then the digital data is regarded as unauthorized data, and therefore digital signature is not added thereto, and the process then proceeds to Step S200.

[0140] If it is determined in Step S206, on the other hand, that the location specified by the location information added as the authentication information of the decrypted digital data is not included in the area within the predetermined range with the location inputted from the location measuring device 54 as the center (No), then the digital data is regarded as unauthorized data, and therefore digital signature is not added thereto, and the process then proceeds to Step S200.

[0141] If it is determined in Step S204, on the other hand, that the time lag between the time specified by the time information added as the authentication information of the decrypted digital data and the time inputted from the time measuring device 52 is not within the predetermined range (No), then the digital data is regarded unauthorized data, and therefore digital signature is not added thereto, and the process then proceeds to Step S200.

[0142] If it is determined in Step S200, on the other hand, that the digital data is not inputted through the communication device 24 (No), then the process remains in Step S200 until digital data is inputted.

--- omission ---

Figure 1

100:	information authentication device
12:	personal information input device
14:	personal information memory unit
16:	digital camera
18:	device information memory unit
18	communication device
20	data memory unit
22	output terminal
40	information processing device
42	time measuring device
44	location measuring device
46	user authentication device
200	authentication authority
24	communication device
26	personal information memory unit
28	device information memory unit

50 information processing unit
52 time measuring device
54 location measuring device

Fig. 3

S100 output user's request for authentication
S102 user authorized?
S104 digital data inputted?
S106 generate time information
S108 generate location information
S110 generate environmental condition information
S112 read out personal information from personal information memory unit
S114 read out device information from device information memory unit
S116 add time information, location information, environmental condition information, personal information, and device information to digital data as authentication information
S118 generate test information by hash function
S120 add test information to digital data as authentication information
S122 encrypt digital data with authentication information added with secret key of information authentication device
S124 transmit digital data to authentication authority
S126 any digital data received from authentication authority?
S128 store digital data in data memory unit
S130 any request for outputting digital data?
S132 output digital data of data memory unit to output terminal
S134 shut off electric power supply forcibly

Fig. 5

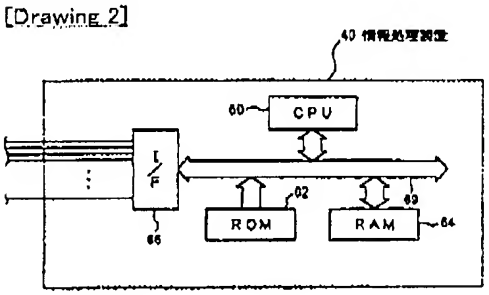
S200 digital data received?
S202 decrypt received digital data with public key of information authentication device
S204 time lag within predetermined range?
S206 location within predetermined area?
S208 decrypt device information
S210 search device information memory unit for device information
S212 device information retrieved?
S214 decrypt personal information
S216 read out personal information from personal information memory unit
S218 personal information matched?
S220 generate test information by hash function
S222 test information matched?
S224 add digital signature to digital data
S226 encrypt digital data with digital signature added with secret key of authentication authority
S228 transmit digital data to information authority device

* NOTICES *

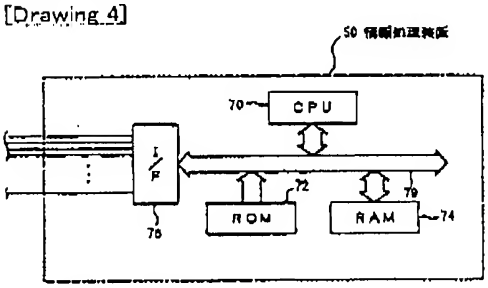
1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DRAWINGS

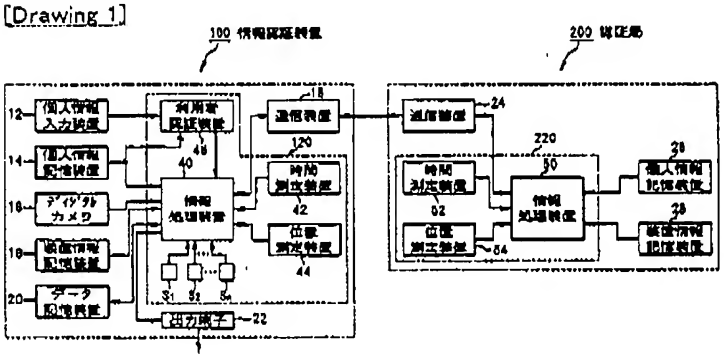
[Drawing 2]



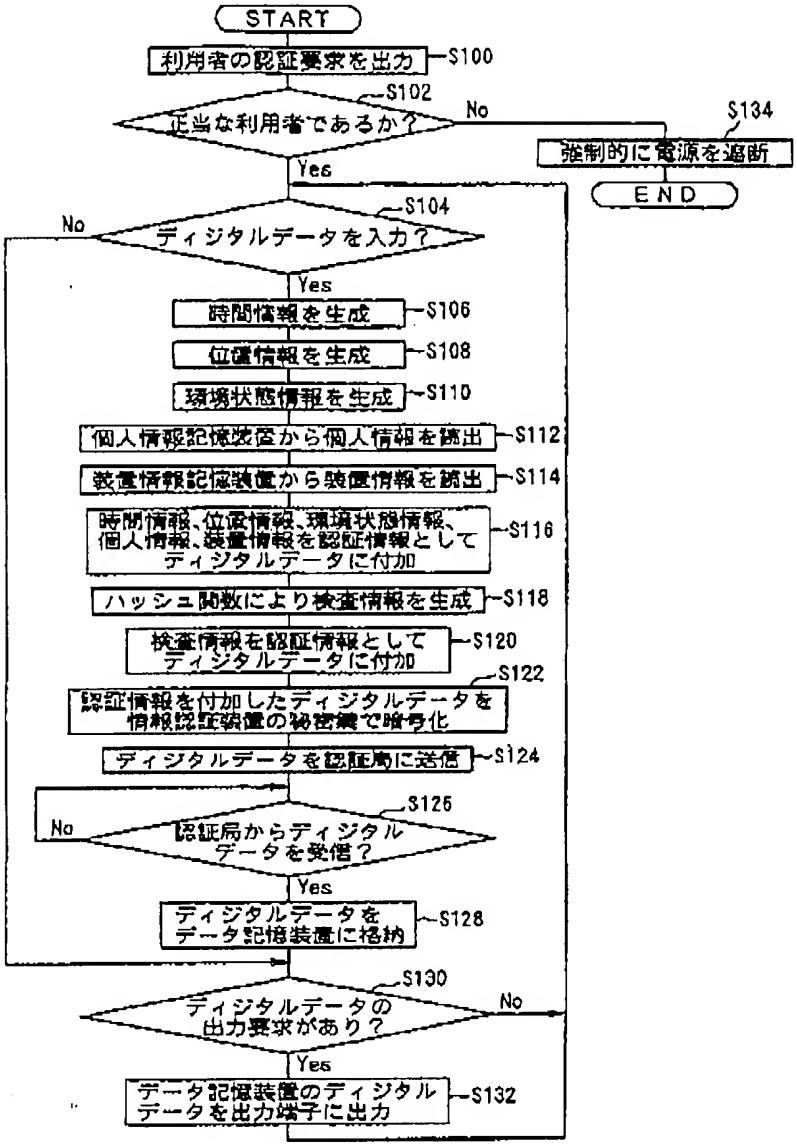
[Drawing 4]



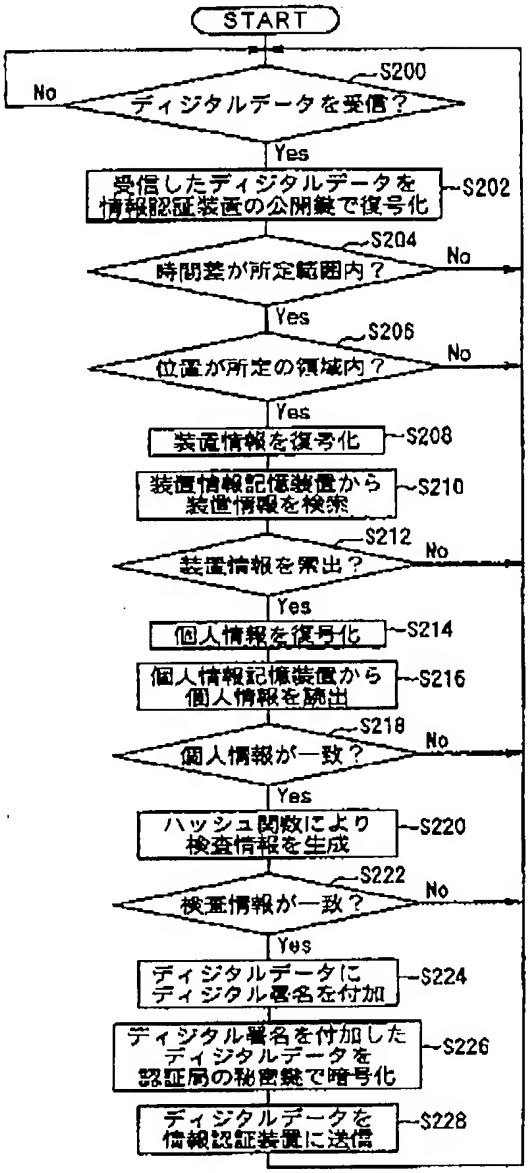
[Drawing 1]



[Drawing 3]


START
利用者の認証要求を出力
S100
S102
正当な利用者であるか？
No
S134
強制的に電源を遮断
END
Yes
S104
No
ディジタルデータを入力？
Yes
時間情報を生成
S106
位置情報を生成
S108
環境状態情報を生成
S110
個人情報記憶装置から個人情報を読出
S112
装置情報記憶装置から装置情報を読出
S114
時間情報、位置情報、環境状態情報、
個人情報、装置情報を認証情報として
ディジタルデータに付加
S116
ハッシュ関数により検査情報を生成
S118
検査情報を認証情報として
ディジタルデータに付加
S120
S122
認証情報を付加したディジタルデータを
情報認証装置の秘密鍵で暗号化
ディジタルデータを認証局に送信
S124
S126
No
認証局からディジタル
データを受信？
Yes
ディジタルデータを
データ記憶装置に格納
S128
S130
ディジタルデータの
出力要求があり？
No
Yes
データ記憶装置のディジタル
データを出力端子に出力
S132

[Drawing 5]



[Translation done.]